

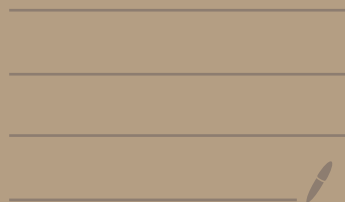
Vorlesung 4

* (Abstrakte) Gruppen (1.5)

1.5.2: Die Menge der rationalen Zahlen $\mathbb{Q}$

2.1: Das abstrakte Konzept von
angeordnetem Körper

Bis zum $\rightarrow$ Satz 2.14 "Bernoullische
Ungleichung"



Vom letzten Mal...

Definition 1.5.2

Es sei G eine Menge und $*$: $G \times G \rightarrow G$ eine zweistellige Verknüpfung. Dann ist das Paar $(G, *)$ eine **Gruppe**, falls

- (1) $*$ assoziativ ist;
- (2) es ein Element $e \in G$ gibt, das **neutrales Element** genannt wird, das erfüllt

$$e * g = g * e = g \quad \text{für alle } g \in G;$$

- (3) jedes Element $g \in G$ ein **inverses Element** besitzt, das mit g^{-1} bezeichnet wird, nämlich ein Element, für das gilt

$$g * g^{-1} = g^{-1} * g = e.$$

Falls die Verknüpfung kommutativ ist, dann wird $(G, *)$ **kommutative Gruppe** genannt.

Lemma: $(\mathbb{Z}, +)$ ist eine (kommutative) Gruppe

$(\mathbb{N}, +)$ $\left. \begin{array}{l} + \text{ assoziativ} \\ 0 \text{ neutrales Element} \end{array} \right\}$ Monoid

$\forall n \neq 0 \quad \nexists m \in \mathbb{N} : n + m = 0$

$$\begin{aligned} \underline{\text{Bmh}} : \quad & [(n, 0)] \stackrel{\sim}{\rightarrow} n, \quad \underline{n \in \mathbb{N}} \\ & [(0, n)] \stackrel{\sim}{\rightarrow} -n, \quad \underline{\text{"}} \\ & [(0, 0)] \rightarrow 0 \end{aligned}$$

$m + (-n)$: wir schreiben $m - n$

(Also : $m - n - p$ bedeutet $m + (-n) + (-p)$)

$$\begin{aligned} \text{"} m - n \text{"} & \stackrel{\sim}{\rightarrow} (m, n) \sim (m', n') \\ & \quad \underline{m - n = m' - n'} \quad \swarrow \searrow \\ & \quad m + n' = m' + n \end{aligned}$$

$$\mathbb{N} \rightarrow \mathbb{Z}$$

$$n \mapsto [(n, 0)]$$

Lemma 1: $(G, *)$ Gruppe. Dann sind
das neutrale Element und
das inverse Element eines (beliebigen)
Element eindeutig bestimmt

Beweis:

1) "e"

$$l_1, l_2 \in G : l_1 * g = g * l_1 = g \quad \forall g \in G$$

$$l_2 * g = g * l_2 = g \quad \forall g \in G$$

$$\underline{l_2} \xrightarrow{\quad} l_1 * l_2 \xrightarrow{\quad} \underline{l_1}$$

$\downarrow$
 l_1
 neutrales
 Element

$\downarrow$
 l_2
 neutrales
 El.

2) $\forall g \in G$, das inverse Element
eindeutig bestimmt

$$\cdot \quad g_1, g_2 \in G$$

$$(i) \quad g_1 * g = g * g_1 = e$$

$$(ii) \quad g_2 * g = \underbrace{g * g_2}_{(i)} = e$$

zu beweisen: $g_1 = g_2$

$$\underline{g_1} = g_1 * e \stackrel{(ii)}{=} g_1 * (g * g_2) =$$

$$\stackrel{\text{Assoziat.}}{=} \underbrace{(g_1 * g)}_{*} * g_2 \stackrel{(i)}{=} e * g_2 = \underline{g_2}$$

Lemma 2: $(G, *)$ eine Gruppe. Dann

1) Für jede $a, b \in G$ hat die Gleichung

$$a * x = b$$

eine eindeutige Lösung, $x = a^{-1} * b$

2) $\forall a \in G, (a^{-1})^{-1} = a$

3) $\forall a, b \in G, (a * b)^{-1} = b^{-1} * a^{-1}$

4) $e^{-1} = e$

Beweis

1) $a * x = b \iff \underbrace{a^{-1} * a}_{e} * x = a^{-1} * b$

$\Downarrow$
 $x = e * x = a^{-1} * b$

2) $\rightarrow \underbrace{a * a^{-1}} = a^{-1} * a = e \leftarrow$

$\Rightarrow a = (a^{-1})^{-1}$

$$3.) (a * b)^{-1} = \underbrace{b^{-1} * a^{-1}}$$

$$(a * b) * (b^{-1} * a^{-1}) \stackrel{z.B.}{=} e$$

|| Assoc.

$$a * (b * b^{-1}) * a^{-1}$$

||

$$(a * e) * a^{-1}$$

||

$$a * a^{-1}$$

||

$$e$$

Bzw

~~$$(a * b)^{-1} = a^{-1} * b^{-1}$$~~

$$4.) \underbrace{e^{-1} = e}$$

$$e * e = e$$



• $\mathbb{Z}$ besitzt eine Multiplikation

$$(m-n) \cdot (m'-n') = m \cdot m' + n \cdot n' - (m \cdot n' + n \cdot m')$$

$\downarrow \quad \forall m, n, m', n' \in \mathbb{N}$

$$\leadsto [(m, n)] \cdot [(m', n')] := [(m m' + n n', m n' + n m')]$$

$$\sim \quad \downarrow \quad [g_1] * [g_2] = [g_1 * g_2]$$

$g'_1 \sim g_1, g'_2 \sim g_2$, ist es wahr, dass $g'_1 * g'_2 \sim g_1 * g_2$?

Aber... was sollten wir noch prüfen?

• Bwk: $(A)'' 1 = [(1, 0)]$ ist das neutrale
(Übung) Element für $\cdot$

$$[(m, n)] \cdot [(1, 0)] = [(m, n)] = [(1, 0)] \cdot [(m, n)]$$

Übung (1.5.4) (B) Die Multiplikation $^m \mathbb{Z}$ ist
distributiv über der Addition
in $\mathbb{Z}$

$$\textcircled{c) \quad 0 \cdot n = n \cdot 0 = 0 \quad \forall n \in \mathbb{Z}$$

$\downarrow$
 $[0, 0]$

$\downarrow$
 $[(m, 0)]$
 oder
 $[0, m]$

(D) Multiplikation ist assoziativ

• Ist $(\mathbb{Z}, \cdot)$ eine Gruppe?

$$0 \quad n \in \mathbb{Z} \quad n \cdot 0 = 0 \cdot n = 0 \neq 1$$

• Ist $(\mathbb{Z} \setminus \{0\}, \cdot)$ eine Gruppe?

$$\textcircled{\pm 1}$$

$$m \quad m > 0 \quad \forall m > 1 \quad \exists n \in \mathbb{Z} \setminus \{0\} \\ m \cdot n = 1$$

Also, wir können die Gleichungen

$$a \cdot x = b, a, b \in \mathbb{Z} \setminus \{0\}$$

in $\mathbb{Z} \setminus \{0\}$ nicht immer lösen

... Erweiterung von $\mathbb{Z}$

$\leadsto$ Fraktionen $\left[\frac{p}{q} \right]$, $p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\}$

in $\mathbb{Z} \times \mathbb{Z}_0$ ($\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$)

Äquivalenzrelation

$$(p, q) \underset{\uparrow}{\sim} (p', q') \iff p \cdot q' = p' \cdot q$$

$$\frac{q' \cancel{p} \cancel{q'}}{\cancel{q}} = \frac{\cancel{p} \cdot q}{\cancel{q'}}$$

$$\frac{p}{q} = \frac{p'}{q'} \iff p \cdot q' = p' \cdot q$$

Def Die Menge der rationalen Zahlen ist
die Menge der Äquivalenzklassen
 $\mathbb{Z} \times \mathbb{Z}_0 \setminus$
 $\approx$

und wird durch $\mathbb{Q}$ bezeichnet

Notation $\frac{p}{q} := [(p, q)]$
 $\swarrow \searrow$ der Zähler der Nenner

• Summe : $[(p, q)] + [(p', q')] = [(pq' + p'q, qq')]$
 $\uparrow$

$$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'}$$

• Multiplikation $[(p, q)] \cdot [(p', q')] = [(pp', qq')]$
 $\searrow$

$$\frac{p}{q} \cdot \frac{p'}{q'} = \frac{p \cdot p'}{q \cdot q'}$$

Übung 1.5.6

• Warum ist $\mathbb{Q}$ eine Erweiterung von $\mathbb{Z}$?

(i) $\mathbb{Z} \hookrightarrow \mathbb{Q}$ injektiv
 $n \mapsto [(n, 1)] = \frac{n}{1}$

$$\begin{array}{ccc}
 (n, m) & \xrightarrow{\quad} & (i(n), i(m)) \\
 \mathbb{Z} \times \mathbb{Z} & \xrightarrow{i \times i} & \mathbb{Q} \times \mathbb{Q} \\
 \downarrow + \quad \boxed{=} & & \downarrow + \\
 \mathbb{Z} & \xrightarrow{\quad} & \mathbb{Q} \\
 \textcircled{n+m} & \xrightarrow{i} & i(n+m) // i(n) + i(m)
 \end{array}$$

* ist + oder •

Wir definieren:

$$\underline{0} := \left(\frac{0}{n} \right) \left(\frac{0}{n} = \frac{0}{m} \right)$$

① neutrales Elem.
der Addition in $\mathbb{Q}$

$$n \in \mathbb{Z} \setminus \{0\}$$

$$\forall n, m \in \mathbb{Z} \setminus \{0\}$$

$$\underline{1} := \frac{1}{1} = \frac{n}{n}$$

$$n \in \mathbb{Z} \setminus \{0\}$$

↳ neutrales Elem.
der Multipl. in $\mathbb{Q}$

Beak: $0 \cdot \frac{p}{q} = 0 \quad \forall \frac{p}{q} \in \mathbb{Q}$

Ist $(\mathbb{Q}, \cdot)$ eine Gruppe?

$$0 \cdot \frac{p}{q} = 0 \neq 1$$

$$\exists? \frac{p}{q} \in \mathbb{Q} : 0 \cdot \frac{p}{q} = 1 \quad ?$$

Ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ eine Gruppe? (Ja)

1) $\cdot$ ist assoziativ. ✓

2) $\cdot$ besitzt ein neutrales Elem. ✓ 1

3) $\forall \left(\frac{p}{q}\right)^{\overset{g}{=}} \in \mathbb{Q} \setminus \{0\} \quad \exists \left(\frac{p'}{q'}\right)^{\overset{g^{-1}}{=}} \in \mathbb{Q} \setminus \{0\}$

so dass $g \cdot g^{-1} = g^{-1} \cdot g = e$

$$\left(\frac{p}{q}\right)^{-1} = \frac{q}{p}$$

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \left(\frac{p \cdot q}{p \cdot q}\right) = 1 \left(= \frac{1}{1}\right)$$

Satz 1.5.5

Es sei $(\mathbb{Q}, +, \cdot)$ die Menge der rationalen Zahlen, mit den Operationen von Addition und Multiplikation. Dann

- (i) $(\mathbb{Q}, +)$ ist eine kommutative Gruppe mit neutralem Element 0;
- (ii) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1;
- (iii) Die Multiplikation $\cdot$ ist distributiv über der Addition $+$, d.h., dass

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \text{für alle } a, b, c \in \mathbb{Q}.$$

Übung: Distributivität in $\mathbb{N}$
der Multipl. über der Addition

• Ordnung auf $\mathbb{Q}$:

$$\frac{p}{q} \leq \frac{p'}{q'} : \Leftrightarrow (pq' - p'q) \underbrace{(qq')^2}_{\text{Mult. } (qq')^2} \leq 0$$

$$\frac{p}{q} - \frac{p'}{q'} \leq 0 \quad \frac{pq' - p'q}{qq'} \leq 0 \quad \rightsquigarrow$$

2.1 Körper

Definition 2.1.1

Es sei K eine Menge mit mindestens zwei Elementen, zusammen mit den (zweistelligen) Verknüpfungen $+$ (die *Addition* genannt wird) und $\cdot$ (die *Multiplikation* genannt wird). Dann ist das Tripel $(K, +, \cdot)$ ein **Körper**, falls

- (i) $(K, +)$ eine kommutative Gruppe ist (mit neutralem Element 0).
- (ii) $(K \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist (mit neutralem Element 1).
- (iii) Die Multiplikation distributiv über der Addition ist, d.h.

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z), \quad \text{für alle } x, y, z \in K.$$

der vorherige Satz...

$\boxed{(\mathbb{Q}, +, \cdot) \text{ ist ein Körper}}$

• Man definiert

$$\forall x_i \in K$$

$$x_1 + \dots + x_k,$$

$$x_1 \cdot \dots \cdot x_k$$

$$x^{-n} := (x^{-1})^n$$

$$x \in K, n \in \mathbb{N}$$

⚡

Wir erhalten:

$$\underbrace{x^n \cdot x^m}_{\text{}} = \underbrace{x^{n+m}}_{\text{}}$$

$$, \underbrace{(x \cdot y)^n = x^n \cdot y^n}_{\text{}}$$

$$\forall x, y \in K \setminus \{0\}$$

$$\forall n, m \in \underbrace{\mathbb{Z} \setminus \{0\}}_{\text{}}$$

$$\hookrightarrow \underline{x^0 = 1}$$

$$\begin{array}{ccc} x^n \cdot x^{-n} & = & 1 \\ \parallel & & \\ (x^{-1})^n & & \end{array}$$

$\swarrow$
 x^0

Allgemeine Eigenschaften eines Körpers

Es sei $(K, +, \cdot)$ ein Körper:

Lemma 2.1.1 :

$$0 \cdot x = 0 \quad \forall x \in K$$

Beweis :

$$\exists y \in K : 0 \cdot x = y$$

$$\text{Zu bew. } y = 0$$

$$\boxed{\begin{array}{l} (G, *) \text{ Gruppe} \\ g^2 = g \Rightarrow \\ g = e \end{array}}$$

$$y = 0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x = y + y$$

$$\textcircled{y = y + y} \quad (K, +) \Rightarrow y = 0$$

$$\xrightarrow{-y}$$

Bwk : $(K, \cdot)$ ist keine Gruppe!

$$\cdot \text{ Inverse von } 0 ? \quad 0 \cdot x = 0 \neq 1$$

$$\begin{array}{l} -y + y = -y + y + y = y \\ \quad \quad \quad \parallel \\ \quad \quad \quad 0 \end{array}$$

Lemma 2.1.2 :

Notation

$-a$: inverses El. von a bzgl. $+$

a^{-1} " " "

Für beliebige $a, b \in K$:

1. $(K, +, \cdot)$ ist nullteilerfrei :

$$a * b = 0 \Rightarrow a = 0 \text{ oder } b = 0$$

($\Leftarrow$ schon bewiesen)

$$2. \quad a * (-b) \stackrel{\uparrow}{=} - (a * b) \stackrel{\uparrow}{=} (-a) * b =: -a * b$$

Beweis

$$1. \quad a * b = 0 \quad a = 0 \quad \checkmark$$

$$a \neq 0 \quad a \in K \setminus \{0\} \Rightarrow \exists a^{-1} \in K \setminus \{0\}$$

$$b = \overbrace{(a^{-1} * a) * b}^{\text{Lemma}} = a^{-1} * 0 \stackrel{\text{Lemma}}{=} 0$$

$$2. \quad a * (-b) \stackrel{\cdot}{=} - (a * b) \Leftrightarrow$$

$$\text{Zu bew. } (a * (-b)) + a * b = 0$$

$\parallel$ Distr.

$$a * ((-b) + b) = a * 0 \stackrel{\text{Lemma 2.1.1.}}{=} 0$$

Angeordneter Körper

Definition 2.1.2

Es sei $\leq$ eine totale Ordnung auf einem Körper $(K, +, \cdot)$, und $<$ die induzierte Ordnung:

$$a < b : \Longleftrightarrow a \leq b \wedge a \neq b.$$

Dann ist $<$ *verträglich* mit $+$ und $\cdot$, falls für jedes $a, b, c \in K$ gilt:

(i) $a < b \implies a + c < b + c$

(ii) Für $c > 0$, $a < b \implies a \cdot c < b \cdot c$

Ein angeordneter Körper ist ein Körper $(K, +, \cdot)$ zusammen mit einer totalen verträglichen Ordnung $\leq$, und heißt **angeordneter Körper**.

$(\mathbb{Q}, +, \cdot)$ ist ein angeordneter Körper
 $\leq$

Bem: Nicht alle Körper besitzen eine
verträgliche Ordnung!

$$(\mathbb{Z}_2, +, \cdot)$$

$$\mathbb{Z}_2 = \{0, 1\} = \{\underline{0}, \underline{1}\}$$

$$(1+1=0 \dots)$$

$(K, +, \cdot)$ angeordneter Körper

$$\left. \begin{array}{l} \textcircled{*} (i) \quad a < b \iff a+c < b+c \\ \textcircled{*} (ii) \quad c > 0, \quad a < b \Rightarrow a \cdot c < b \cdot c \end{array} \right\} \begin{array}{l} \forall a, b, c \\ \in K \end{array}$$

Lemma 2.1.3.

1. $a > 0 \iff -a < 0$ ^(*) (gilt auch $\geq, \leq$)

$$a > 0 \stackrel{(i)}{\iff} a - a > 0 - a \iff 0 > -a$$

2. $a > b \iff a - b > 0 \iff -b > -a$ (*)

$$a > b \stackrel{(i)}{\iff} a - b > b - b = 0 \iff -a + a - b > 0 - a \\ -b > -a$$

3. Falls $a > 0$ und $b > 0 \Rightarrow a+b > 0$ und $a \cdot b > 0$ (*)

Übung

$(K, +, \cdot)$ angeordneter Körper

$$\left. \begin{array}{l} \text{(i)} a < b \Rightarrow a + c < b + c \\ \text{(ii)} c > 0, a < b \Rightarrow a \cdot c < b \cdot c \end{array} \right\} \begin{array}{l} \forall a, b, c \\ \in K \end{array}$$

4. Falls $a > b$ und $c > d \Rightarrow$ (*)
 $a + c > b + d$

Übung

5. Falls $a > b > 0$ und $c > d > 0 \Rightarrow$ (*)
 $a \cdot c > b \cdot d$

Übung

6. Falls $a < b$ und $c < 0 \Rightarrow a \cdot c > b \cdot c$ (*)
 $c < 0 \Rightarrow -c > 0$

(ii) $\Rightarrow$ weil $a < b \Rightarrow a \cdot (-c) < b \cdot (-c)$

Lemma
 $a \cdot (-c) = -a \cdot c$
 $b \cdot (-c) = -b \cdot c$

$$\leadsto -a \cdot c < -b \cdot c$$

$$\xrightarrow{2.} a \cdot c > b \cdot c$$

□

$(K, +, \cdot)$ angeordneter Körper

$$\left. \begin{array}{l} \text{(i)} a < b \Rightarrow a + c < b + c \\ \text{(ii)} c > 0, a < b \Rightarrow a \cdot c < b \cdot c \end{array} \right\} \begin{array}{l} \forall a, b, c \\ \in K \end{array}$$

7. Falls $a \neq 0$, dann ist $a^2 > 0$

Insbesondere ist $1 > 0$

Übung

8. Die Gleichung $x^2 + 1 = 0$ hat keine Lösung in einem angeordneten Körper

Übung

9. $a > 0 \Rightarrow a^{-1} > 0$

$$a > 0, a \neq 0 \Rightarrow \exists a^{-1} \neq 0 \xrightarrow{7.} (a^{-1})^2 > 0$$

$$[a > 0, (a^{-1})^2 > 0] \xrightarrow{\text{(ii)}} a \cdot (a^{-1})^2 > 0$$

$$10. \text{ Falls } a > b > 0 \Rightarrow \underbrace{b^{-1} > a^{-1}}_{\substack{a \cdot (a^{-1})^2 \\ = a^{-1}}}$$

Übung

Satz 2.1.4

(Bernoullische Ungleichung) Es sei $(K, +, \cdot)$ ein angeordneter Körper und n eine natürliche Zahl. Dann gilt für jedes $x \in K$ mit $1+x \geq 0$ die Ungleichung

$$(1+x)^n \geq 1+n \cdot x.$$

Beweis

Induktionsbeweis

$$P(n) : "(1+x)^n \geq 1+n \cdot x"$$

• Induktionsanfang

$$P(0) \text{ wahr : } \underbrace{(1+x)^0}_{1} \geq 1 + \underbrace{0 \cdot x}_0$$

Induktionsschritt

Angenommen $P(n)$ wahr

IH

$$(1+x)^n \geq 1+nx \quad ((1+x) \geq 0)$$

Zu beweisen:

$$(1+x)^{n+1} \geq 1+(n+1)x$$

$$\underline{(1+x)^{n+1}} = (1+x)^n \cdot (1+x) \geq (1+nx)(1+x)$$

(IH)
IH

$$\boxed{(1+x)^n \geq 1+nx} \quad \text{IH}$$
$$\textcircled{(1+x) \geq 0}$$

$$1 + (n+1)x + nx^2$$

$$1 + (n+1)x + nx^2 \geq 1 + (n+1)x$$

Behauptung

$x \neq 0 \Rightarrow x^2 > 0$ und Lemma 2.1.3, 3.
7.

$$\Rightarrow \underline{nx^2 > 0}$$

$$\circ \quad 1 + (n+1)x + n x^2 \geq 1 + (n+1)x$$

$$4. \Rightarrow 1 + (n+1)x + n x^2 \geq 1 + (n+1)x$$

□